Development of a Fog Miner Based Device Authentication Model in IoT - Blockchain Platform

Piyali Ganguly
A. K. Choudhury School of I.T.
University of Calcutta
Kolkata, India
piyaliganguly1992@gmail.com

***Abstract*—IoT is a system framework comprises several layers such as device layer, fog layer, cloud layer and each layer performs a specific task such as data acquisition, data storing, data processing and report generation. Multi - layer system architecture comprises various IoT devices and each IoT device can communicate with each other by means of data transferring. To perform data communication in between those devices each IoT device needs to be authenticated with each other. Fog computing performs real - time device authentication mechanism. In this paper we have described the device authentication model in fog computing platform using blockchain technology by mitigating several IoT based threat scenarios.**

***Index Terms*—Fog node, Miner node, IoT, Blockchain, Device authentication.**

I. Introduction

The present state of the art of IoT security comprises several areas such as device authentication, end to end data encryption using lightweight cryptography, lightweight cryptographic protocol based mutual authentication between two devices and data security. IoT based system architecture consists of several layers such as device layer, fog layer and cloud layer. Each layer is composed of several IoT devices which perform data acquisition and data processing inside them. To perform data communication between each of IoT devices each device needs to be authenticated with each other. Device authentication in IoT domain can be done in many ways and device authentication approaches can be subdivided in to two parts such as real−time system based device authentication approaches and remote server based approaches.

In real−time system each IoT devices are authenticated using a trusted local server [1] - [4]. IoT device equipped with physical unclonable function (puf) can be authenticated using a trusted local server. Device to device authentication can be performed using lightweight protocols [5] - [7]. IoT devices can be authenticated using distributed consensus mechanism, where a single trusted third party (ttp) is eliminated using multiple miner blocks [9]-[10]. Consensus protocol is a part of blockchain technology and consensus mechanism based device authentication is the new trend in IoT domain. Consensus protocol requires a large amount of computations inside a miner block and several inter miner data communications. IoT devices are resource constrained and the implementation of consensus based device authentication in fog level is a challenging issue in IoT domain. Centralised remote server based device authentication is another domain in IoT based system. In IoT based system framework, cloud platform is assumed as a trusted global server. Inside a cloud platform an one-time password (OTP) can be generated and that OTP will be send to the IoT node for performing device authentication. In many cases OTP based IoT device authentication [8] is performed and in those cases cloud is considered as a centralised ttp. IoT and cloud blockchain based device authentication is another part of this research work and here miner blocks reside at cloud platform. Cloud blockchain based [11] device authentication approach is not a real−time technique. Several works have performed based on cloud blockchain technology. Attribute based encryption (ABE) [12] in addition with blockchain technology is performed in [12]. ABE scheme can perform authentication as well as encryption simultaneously. ABE scheme integrated with blockchain architecture eliminates the concept of centralised ttp. In [13] - [14] lightweight blockchain based consensus protocol is described. In [13] - [14] the reverse hash calculation is eliminated and a lightweight consensus mechanism is described.

The main research challenges in this context is to develop a real−time device authentication approach in fog layer and to estimate the upper bound of required miner nodes to validate an IoT node corresponding to a particular fog node. Here, we have outlined this problem statement and the design approaches to solve that problem by analysing various parameters of this model such as

- Upper bound of the number of fog nodes waiting in the system.
- Upper bound of waiting time for each of the fog nodes to access the miner node.

The rest of the paper is organised as follows: section 2 describes methodology of this concept, section 3 presents experimental setup and analysis, section 4 concludes the paper.

II. Methodology

A. System Architecture

This framework is composed of several IoT layers such as device layer, fog layer, miner layer and cloud layer.

Device layer: This layer is composed of several IoT nodes and each node is constructed with data acquisition unit, communication module and sensors. IoT nodes acquire data

from sensing objects and transfer those data to the fog layer.
Fog layer: This layer is composed of several fog nodes and perform data storing, processing and report generation inside it.
Miner layer: This is another kind of fog layer where each fog node is considered as a trusted node. This miner layer can function parallel according to the fog layer. This layer contains miner nodes as well as administrative nodes.
Cloud layer: Cloud layer performs as a global data storage.

B. Threat Scenarios:

To design blockchain based security framework first we have designed several threat scenarios such as:
Case 1: IoT node is untrusted and fog node is trusted.
Case 2: IoT node is trusted and fog node is untrusted.
Case 3: IoT node is and fog node both are untrusted.
Case 4: Miners information can be eavesdropped.

C. Threat Modelling:

To model the threat scenarios let us assume that $S1 = \{IoT\_node_1, IoT\_node_2, IoT\_node_3, Fog\_node_1\}$ and $S2 = \{IoT\_node_4, IoT\_node_5, IoT\_node_6, Fog\_node_2\}$ are the two fog models, consisting of several IoT nodes and one fog node. Each S_1 and S_2 performs data acquisition, data storing and data processing inside them. Here, each IoT node can communicate with a particular fog node. To perform data communication with a particular fog node, an IoT node can send a request to the fog node without knowing that the request is received by a valid fog node. If the fog node is not a valid fog node or the id of the IoT node is forged by any other malicious IoT node then sensor data will be dropped. Algorithm 1 describes the threat modelling part of this work.

D. Threat Mitigation:

Threat mitigation is a step where probable threats can be detected and will be mitigated through threat mitigation algorithm. In Algorithm 1 we have described the threat scenarios which can make the system vulnerable and in Algorithm 2 we have mentioned our proposed concept to mitigate those threat scenarios. Here, we have described the threat mitigation algorithm in three steps such as:

- IoT_node to Fog_node based one way authentication.
- Fog_node to Miner_node based Fog_node authentication.
- Miner_node based IoT_node authentication.
- Finally connection establishment between IoT_node and Fog_node.

E. Threat Model Validation:

In this paper we have described threat scenarios in Algorithm 1 and it's mitigation approach in Algorithm 2. After designing this threat model we have validated this model based on several threat scenarios which are mentioned in Threat Scenarios section.

Algorithm 1 Threat Modelling

Initialization:

- Let, S_1 and S_2 are two fog models.
- $S1 = \{Iot\_node_1, IoT\_node_2, IoT\_node_3, Fog\_node_1\}$
- $S2 = \{IoT\_node_4, IoT\_node_5, IoT\_node_6, Fog\_node_2\}$
- node.unregistered = node is an unregistered node.
- node.registered = registered node.
- node.false = A fake node which contains the id of an authentica node.
- Let, I_x is an unknown IoT node wants to communicate with a fog model.
- Inode = IoT_node
- Fnode = Fog_node
- Inode.registered = registered IoT node.
- fnode.registered = registered fog node.

if (I_x==Inode.registered) **then**
  if (Inode.registered==node.false) **then**
    " Authentication required"
    if (Inode.registered==True) **then**
      if (Fnode.registered==node.false) **then**
        " Authentication of a Fog node is required"
      end if
    end if
  end if
end if
if (I_x==node.unregistered) **then**
  "I_x can't send data"
end if

III. Experimental Setup and Analysis

In our experimental setup we have implemented a hierarchical system architecture which has different IoT layers such as device layer, fog layer, miner layer and cloud layer. Device layer consists of several IoT nodes and each IoT node is composed of several sensors, data acquisition unit and communication module. We have used Arduino uno R3 as a data acquisition unit and it is equipped with temperature and humidity sensor (DHT11), RGB colour sensor, MQ135 gas sensor, LDR sensor and Bluetooth (Hc 05) module to perform data acquisition and data communication in between IoT nodes and fog nodes. We have used smart phone app as a gateway device. Smart phone app acts as a fog node and transfers data to the miner node. Our framework is composed of several fog nodes and miner nodes, here, we have used Raspberry pi 3 B+ model as a miner device. To perform peer to peer data communication in between miner nodes we have used zigbee communication protocol and to transfer data from fog node to cloud platform we have used wifi data communication. We have also built a device to device network where number of IoT nodes can communicate with each other using Bluetooth communication protocol. In this system framework we have used amazon AWS cloud platform as global data storage.

In this paper we have proposed a device authentication model in IoT - Blockchain platform. We have assumed that

Algorithm 2 Threat Mitigation

Initialization:

- UID = Unique ID of every IoT_node and every Fog_node.
- $Send\_request()$ contains Hash(UID, Sig)
- Root_Hash = Hash(UID, Sig)
- Send_verification() contains One_Time_Password (OTP) given by trusted miner node.
- Send_Certificate() contains signed miner's report about IoT_node.
- Send_authentication_report() contains signed certificate of fog_node and miner_node.

Inside IoT node:

- $IoT\_node_{Send\_request()} \rightarrow Fog\_node.$

Inside Fog node:

- $Hash^{'}$ = Hash(UID, Sig)
- **if** ($Hash^{'}$ == root_Hash) **then**
  "IoT node is OK and granted for miner validation"
- **end if**

Inside Mine node:

- $Miner\_node_{Send\_verification()} \Rightarrow IoT\_node$
- **Inside IoT node:**
- $Hash^{''} = Hash(UID, OTP)$
- $IoT\_node(Hash^{''}) \Rightarrow Miner\_node$

Inside Miner node:

- **if** ($Hash^{''} == Hash^{'''}$) **then**
  "IoT node is authenticated"
- **end if**
- $Miner\_node_{Send\_Certificate} \Rightarrow fog\_node$

Inside Fog node

- $Fog\_node_{Send\_authenticatiob\_report} \Rightarrow IoT\_node$
- Fog node accepts data from IoT node

each of the IoT_node and fog_node contains an unique Id which named as UID. AS each of the participating IoT_node and fog_node contains UID then there is no chance of the happening of sybill attack. We have validated our attack mitigation model using various test cases and we can formulate the upper bound of number of fog nodes waiting in the system.

IV. Conclusion

In this paper we have formulated our research problem and developed our proof of concept based on threat scenarios and threat mitigation algorithm. Our future plan is to show the scalability of the blockchain network and to analyse various parameters such as upper bound of the waiting time for each of the fog node in the system and also the number of fog nodes get service from the miner node.

V. Acknowledgement

I sincerely thank to my supervisor Dr. Amlan Chakrabarti, Dean, Faculty of Engineering and Technology, Professor and Director of A.K. Choudhury School of I.T. of University of Calcutta, for his guidance, support and encouragement. I also thank to Prof. Anjan Dasgupta, for his support and guidance. This project has been carried out to the project funding of MeitY, Govt of India.

References

[1] M. N. Aman, K. C. Chua, and B. Sikdar, Mutual authentication in iot systems using physical unclonable functions," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1327-1340, 2017.

[2] U. Chatterjee, V. Govindan, R. Sadhukhan, D. Mukhopadhyay, R. S. Chakraborty, D. Mahata, and M. M. Prabhu, Building puf based authentication and key exchange protocol for iot without explicit crps in verifier database," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 3, pp. 424-437, 2018.

[3] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, A puf-based secure communication protocol for iot," ACM Transactions on Embedded Computing Systems (TECS), vol. 16, no. 3, p. 67, 2017.

[4] P. Gope and B. Sikdar, Lightweight and privacy-preserving two-factor authentication scheme for iot devices," IEEE Internet of Things Journal, vol. 6, no. 1, pp. 580-589, 2018.

[5] L. Zhou, C. Su, and K.-H. Yeh, lightweight cryptographic protocol with certificateless signature for the internet of things," ACM Transactions on Embedded Computing Systems (TECS), vol. 18, no. 3, p. 28, 2019.

[6] L. Zhou, C. Su, Z. Hu, S. Lee, and H. Seo, Lightweight implementations of nist p-256 and sm2 ecc on 8-bit resource-constraint embedded device," ACM Transactions on Embedded Computing Systems (TECS), vol. 18, no. 3, p. 23, 2019.

[7] P. Gope, Laap: Lightweight anonymous authentication protocol for d2d-aided fog computing paradigm," Computers and Security, 2019.

[8] V. Shivraj, M. Rajan, M. Singh, and P. Balamuralidhar, One time password authentication scheme based on elliptic curves for internet of things (iot)," in 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), pp. 1-6, IEEE, 2015.

[9] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6-14, 2018.

[10] O. Novo, Blockchain meets iot: An architecture for scalable access management in iot," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, 2018.

[11] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, Bubbles of trust: A decentralized blockchain-based authentication system for iot," Computers and Security, vol. 78, pp. 126-142, 2018.

[12] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, Privacy-preserving blockchain based iot ecosystem using attribute-based encryption," in 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, IEEE, 2017.

[13] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, Proof-of-authentication for scalable blockchain in resource-constrained distributed systems, in 2019 IEEE International Conference on Consumer Electronics (ICCE), pp. 15, IEEE, 2019.

[14] D. Puthal and S. P. Mohanty, Proof of authentication: Iot-friendlyblockchains, IEEE Potentials, vol. 38, no. 1, pp. 2629, 2018.